PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04Q 7/32

A2

(11) Internationale Veröffentlichungsnummer: **WO 98/57510**

(43) Internationales Veröffentlichungsdatum: 17. Dezember 1998 (17.12.98)

(21) Internationales Aktenzeichen: PCT/DE98/01516

(22) Internationales Anmeldedatum: 3. Juni 1998 (03.06.98)

(30) Prioritätsdaten:
197 24 901.9 12. Juni 1997 (12.06.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS NIXDORF INFORMATIONSSYSTEME AG [DE/DE]; Heinz-Nixdorf-Ring 1, D-33106 Paderborn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: WIEHLER, Gerhard [DE/DE]; Am Bogen 43, D-82223 Eichenau (DE).

(74) Gemeinsamer Vertreter: SIEMENS NIXDORF INFORMATIONSSYSTEME AG; Epping, Wilhelm, Postfach 22 13 17, D-80503 München (DE).

(81) Bestimmungsstaaten: CA, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

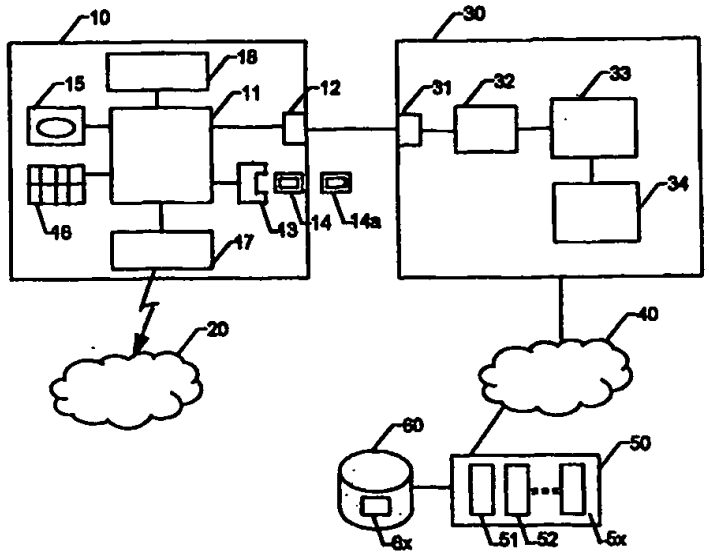
Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: TELECOMMUNICATION AND/OR REMOTE CONTROL DEVICE WITH A CHIP CARD UNIT, SAME DEVICE WITH A COUPLED COMPUTER FOR INTERNET OR NETWORK APPLICATIONS AND METHOD FOR OPERATING SUCH A COMBINATION OF DEVICES

(54) Bezeichnung: GERÄT DER TELEKOMMUNIKATIONS- UND/ODER FERNSTEUERTECHNIK MIT CHIPKARTENEINHEIT SOWIE SOLCHE MIT GEKOPPELTEM RECHNER FÜR INTERNET- BZW. NETZANWENDUNGEN UND VERFAHREN ZUM BETREIBEN EINER SOLCHEN GERÄTEKOMBINATION

(57) Abstract

A chip card unit (13) pertaining to a mobile radio telephone, for instance, is connected to an interface (12) for a computer via a control unit (11) enabling the mobile radio telephone (10) to operate as a card terminal when coupled to a computer (30). When the computer (30) is connected to a telecommunication network (40), occupation of network services by service providers (50) is also possible. Chip card applications include mutual client-server authentication, verification of access rights, digital signature for sensitive data, generation of keys to encrypt data, proof of ordering, payment from an electronic purse, etc.



(57) Zusammenfassung

Anschluß der Chipkarteneinheit (13) z.B. eines Mobilfunktelefons (10) als Gerät über eine Steuereinheit (11) an die Anschlußschnittstelle (12) für einen Rechner (30), so daß das Mobilfunktelefon (10) bei Kopplung mit einem Rechner (30) als Kartenterminal betreibbar ist. Ist der Rechner (30) an ein Kommunikationsnetz (40) angeschlossen, dann ist auch eine Inanspruchnahme der Netzdienste von Dienstanbietern (50) möglich. Chipkartenanwendungen z.B. für die gegenseitige Client-Server-Authentisierung, für die Verifikation von Zugriffsrechten, für die digitale Signatur sensibler Daten, für die Erzeugung von Schlüsseln zur Verschlüsselung von Daten, für den Beweis eines Bestellvorganges, für die Bezahlung aus einer elektronischen Börse usw.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Gerät(10) der Telekommunikations- und/oder Fernsteuertechnik mit Chipkarteneinheit sowie solche mit gekoppeltem Rechner für Internet- bzw. Netzanwendungen und Verfahren zum Betreiben einer solchen Gerätekombination

Die Erfindung betrifft Anordnungen und Verfahren für die Nutzung von im Internet oder in anderen Netzen angebotenen Leistungen, die hohe Sicherheitsanforderungen stellen.

Geräte mit Chipkarteneinheit sind z. B. Mobilfunktelefone, die im wesentlichen für die Sprachübertragung in Mobilfunknetzen benutzt werden. Das im Mobilfunktelefon integrierte sogenannte SIM-Modul bzw. die integrierte Chipkarte dient zur Authentisierung des Mobilfunktelefons als ein für den Mobilfunk berechtigtes Gerät und enthält Schlüssel für die Verschlüsselung der ausgesandten Sprachinformation bzw. für die Entschlüsselung der empfangenen Sprachinformation.

Eine andere Art von Geräten mit Chipkarteneinheit bilden z.B. Fernsteuerungen für Fernsehgeräte, bei denen zum Empfang von kostenpflichtigen Fernsehsendungen die Chipkarte als Berechtigungsnachweis und gegebenenfalls auch als Zahlungsmittel dient.

Rechner, wie z.B. Personalcomputer oder Laptops, die einen Festnetz- oder Mobilnetzanschluß aufweisen, sind in der Lage, z.B. mittels http-Protokoll, Internetanwendungen zu nutzen. Bei besonders sicherheitsrelevanten Vorgängen, wie z.B. bei Bestellungen und Zahlungen, werden Chipkarten verwendet, die über einen am Rechner angeschlossenen Chipkartenleser die jeweiligen Transaktionen steuern. Die Verbindung mit einem Mobilfunknetz kann dabei auch über ein mit einem Datenanschluß-ausgerüsteten Mobilfunktelefon erfolgen - man siehe z.B. „PC Professionell", März 1994, Seiten 253-260 oder „Cash Flow", 2/95, Seiten 140,141.

Weiterhin ist es durch DE 195 38 842 A1 bereits bekannt, über den Datenanschluß zum Mobilfunktelefon Konfigurations- bzw. Gesprächsteilnehmerdaten an einen Speicher im Mobilfunktelefon zu übertragen, wobei auch der Speicher auf dem Chip der Teilnehmerkarte verwendet werden kann. Ebenso können diese im Mobilfunktelefon abgespeicherten Daten an den so angeschlossenen Rechner gelesen und geändert werden.

Auch sind bereits Gerätekombinationen aus Fernseher und Rechner bekannt, bei denen der einzige Bildschirm vom Fernsehteil und vom Rechnerteil gemeinsam genutzt wird.

Mögliche Anwendungen eines Rechners in Verbindung mit einer Chipkarte sind z.B. Authentisierung, Erzeugung von digitalen Signaturen, Kredit-/Debitkartenanwendungen, elektronische Geldbörse.

Eine besonders hohe Sicherheit kann durch asymmetrische kryptographische Verfahren erreicht werden, bei denen der private Schlüssel in der Chipkarte nicht auslesbar gespeichert ist und entsprechende Krypto-Verfahren in der Chipkarte nicht manipulierbar durchgeführt werden. Chipkarten-Bausteine für derartige Anwendungen sind heute auf dem Markt verfügbar, z.B. der Baustein SLE 44CR80S der Siemens AG.

Aufgabe der Erfindung ist es, den Anwendungsbereich der Geräte mit Chipkarteneinheit so zu erweitern, daß in Verbindung mit einem Rechner gesicherte Transaktionen möglich sind.

Dieses wird einerseits gemäß Anspruch 1 dadurch erreicht, daß das Gerät in der Weise erweitert wird, daß es zusätzlich als Kartenterminal für einen Rechner verwendbar ist. Dadurch können auf dem Rechner vorhandene geschützte Dienste in Anspruch genommen werden.

Weiterhin ermöglicht die Verwendung eines solchen erweiterten Gerätes gemäß Anspruch 2 in Verbindung mit einem angekoppelten Rechner, der in bekannter Weise an ein Kommunikationsnetzwerk angeschlossen ist, daß persönliche oder öffentliche Netzdienste, z.B. über das Internet, in Anspruch genommen werden können, die an die Sicherheit hohe Anforderungen stellen, ohne daß die Rechner über Chipkarten-Leseeinrichtungen verfügen müssen. Für Mobilfunktelefon-Inhaber ergibt sich dabei der große Vorteil, daß sie ortsunabhängig von jedem beliebigen Standard-Rechner aus die Netzdienste in Anspruch nehmen können.

Weiterbildungen der Erfindung beziehen sich auf Verfahren zum Betreiben einer derartigen Gerätekombination. Diese betreffen u.a. das Betriebsbereitschalten des als Kartenterminal dienenden Gerätes, das neben der Abwicklung von Netzdiensten in der üblichen Weise auch Verschlüsselungen bzw. Entschüsselungen in an sich bekannter Weise ermöglicht.

Besondere Vorteile ergeben sich daraus, daß hochsensible Daten, wie z.B. die persönliche Geheimzahl PIN oder Geldbeträge am Gerät mit der Tastatur eingegeben und bei vorhandener Anzeige unverschlüsselt angezeigt werden können, bevor sie verschlüsselt an den Rechner weitergeleitet werden. Damit werden Eingaben über die Rechnertastatur vermieden, so daß Viren im Rechner die Eingaben nicht verfälschen können.

Auch besteht in vorteilhafter Weise die Möglichkeit, Kontrollwörter über ein vorhandenes Mikrofon als Berechtigungsnachweis einzugeben, die dann digitalisiert an eine Kontrollinstanz im Kommunikationsnetz weitergeleitet und mit einem Referenzmuster verglichen werden. Auf diese Weise kann die Identität eines Benutzers zusätzlich anhand eines persönlichen biometrischen Merkmales verifiziert werden, was erhöhten Sicherungsanforderungen gerecht wird.

Weiterhin können auch Daten und/oder Steuerinformationen vom Rechner über die Anschlußschnittstelle an den Speicher im Gerät übertragen und dort abgespeichert werden. Damit ist es möglich, Daten auf der Chipkarte zu ändern oder zu speichern. Bei diesen Daten kann es sich z.B. um Schlüssel für die Verschlüsselung bzw. Entschlüsselung oder um einen Geldbetrag für eine Geldkarte handeln. Letztere eröffnet z.B. in Verbindung mit einem Mobilfunktelefon als Gerät die Möglichkeit eines Kartentelefons, indem beim Betrieb als Telefon ankommende Gebührenimpulse eine Abbuchung des jeweils entsprechenden Geldbetrages bewirken.

Einzelheiten der Erfindung seien nachfolgend anhand eines in der Zeichnung dargestellten Ausführungsbeispieles, bei dem als Gerät mit Chipkarteneinheit ein Mobilfunktelefon vorgesehen ist, näher erläutert. Im einzelnen zeigen

FIG 1 eine schematische Übersicht eines Rechners mit Netzkopplung und angeschlossenem Mobilfunktelefon als Kartenterminal für die Inanspruchnahme von Netzdiensten und

FIG 2 eine schematische Darstellung einer Chipkarte für verschiedene Anwendungen.

Bei der Darstellung von FIG 1 ist ein Mobilfunktelefon 10 als Gerät mit Chipkarteneinheit über eine Standardschnittstelle 12, z. B. RS232, an einen Rechner 30 in Form eines üblichen PC angeschlossen. Die Schnittstelle 12 ist innerhalb des Mobilfunktelefons 10 mit einer Steuereinheit 11 verbunden, an die außerdem eine Kontaktiereinheit 13 für das SIM-Modul/die Chipkarte 14/14a, eine Anzeige 15, eine Tastatur 16, ein Sprach- und Funkmodul 17 sowie ein Speicher 18 angeschlossen ist. Das Sprach-und Funkmodul 17 hat dabei in üblicher Weise Zugang zum Mobilfunknetz 20.

Vom Rechner 30 sind lediglich die Anschlußschnittstelle 31 für das Mobilfunktelefon 10 mit dem zuständigen Treiber 32 gezeigt sowie ein sogenannter Browser 33 und Rechneranwendungen 34 für die Inanspruchnahme von Netzdiensten, beispielsweise im Internet,angedeutet, die über das Kommunikationsnetz 40 in Verbindung mit einem entsprechenden Anbieter 50, z.B. in Form eines sogenannten Servers, ausgeführt werden können.

Auf dem SIM-Modul oder der Chipkarte 14 bzw. 14a sind die mit Schlüssel zugänglichen Anwendungen gespeichert. Für die verschiedenen Anwendungen können individuelle Chipkarten vorgesehen werden. Es können aber auch, wie FIG 2 zeigt, die Mobilfunk-Anwendungen für GSM/DCS 141 sowie die verschiedenen Internet-/Netzanwendungen 142, 143, 14x mit ihren unterschiedlichen Schlüsseln auf einer Chipkarte gespeichert sein.

Vor Nutzung eines der Netzdienste ist eine entsprechende Chipkarte auszuwählen und in die Kontaktiereinheit 13 des mit dem Rechner 30 gekoppelten Mobilfunktelefons 10 einzusetzen. Außerdem ist der das Mobilfunktelefon 10 als Kartenterminal über die Anschlußschnittstelle 31 steuernde Treiber 32 mit der entsprechenden Treibersoftware zu laden. Dies kann von einer Diskette aus erfolgen. Um jedoch Manipulationen am Treiber 32 auszuschließen, ist es zweckmäßig, daß die z.B. mit einem privaten Schlüssel des Mobilfunknetz-Betreibers signierte Treibersoftware von einem entsprechenden Server auf Anforderung vom Rechner 30 aus über das Kommunikationsnetz 40 in den Treiber 32 geladen wird. Danach kann dann automatisch eine Verifikation der Treibersoftware anhand eines entsprechenden und sich auf der Chipkarte 14/14a in einem Anwendungsbereich, z. B. 14x, befindlichen öffentlichen Schlüssel des Mobilfunknetz-Betreibers durchgeführt werden.

Die Treibersoftware arbeitet zweckmäßig entsprechend einem bereits festgelegten Standard, wie z. B. ISO 7816-3 und der von der PC/SC-Workgroup gemeinsam mit Microsoft festgelegten ICC Spezifikation (http//:www.smartcardsys.com).

Die Netzanwendung kann im Rechner 30, beispielsweise durch Aufrufen des Browsers 33 und Eingabe eines sogenannten „uniform resource locator" URL gestartet werden. Damit wird über das Netz 40 eine Verbindung zum Dienstanbieter 50 aufgebaut, und es können die gewünschten Dienste 51, 52, .., 5x in Anspruch genommen werden. Das angeschlossene Mobilfunktelefon 10 bzw. die Steuereinheit 11 verhält sich dabei wie ein übliches Kartenterminal. Abhängig von den vom Dienstanbieter 50 bereitgestellten Diensten 51, 52, .., 5x sind Chipkartenanwendungen 142, 143, ...,14x auswählbar und ausführbar, z. B. für die gegenseitige Client-Server-Authentisierung, für die Verifikation von Zugriffsrechten, für die digitale Signatur sensibler Daten, für die Erzeugung von Schlüsseln zur Verschlüsselung von Daten, für den Beweis eines Bestellvorganges, für die Bezahlung aus einer elektronischen Börse.

Gegenüber einem herkömmlichen Chipkartenleser ermöglicht die Erfindung zusätzliche Funktionen, die eine erheblich höhere Sicherheit gewährleisten:

Am Internet angeschlossene Rechner sind prinzipiell aus dem Internet eingeschleusten Viren ausgesetzt. So kann z. B. ein Kontoüberweisungsbetrag, der über die Rechnertastatur eingegeben wird, durch einen solchen Virus verfälscht werden, bevor die Transaktion mit dem Internetserver korrekt abgeschlossen ist.

Mit einem Mobilfunktelefon oder einem anderen Gerät als Kartenterminal kann diese Manipulation dadurch verhindert werden, daß von der Rechner-/Server-Anwendung veranlaßt wird, sensible Daten, wie z. B. Überweisungsbeträge, über die Tastatur 16 des Gerätes 10 einzugeben. Der Steuereinheit 11 wird dies über einen Code mitgeteilt, wodurch die eingegebenen Daten einerseits an der Anzeige 15 unverschlüsselt wahrgenommen und überprüft werden können. Andererseits werden diese Daten durch eine Chipkartenanwendung 14x verschlüsselt

oder signiert und an den Rechner 30 bzw. den zuständigen Server zur weiteren Verarbeitung übergeben.

In gleicher Weise kann bei Eingabe einer persönlichen Geheimzahl PIN, welche durch eine Rechner-/Netz-Anwendung angefordert wurde, die an der Tastatur 16 eingegebene PIN in der Chipkarte verschlüsselt werden, bevor sie an die Rechner-/Netz-Anwendung weitergeleitet wird.

Anwendungen mit höchsten Sicherheitsanforderungen erfordern oftmals eine Authentisierung auf Basis biometrischer Merkmale. Mit der hier dargestellten Erfindung läßt sich dies folgendermaßen realisieren:

Eine Anwendung 5x fordert nach erfolgreicher gegenseitiger Client-Server-Authentisierung auf Basis asymmetrischer Krypto-Verfahren den Benutzer als sogenannten Client auf, eine Sprechprobe abzugeben, z. B. ein vereinbartes Kennwort dreimal hintereinander in das Mikrofon 17 des Mobilfunktelefons 10 zu sprechen. Die Steuereinheit 11 leitet dann, beispielsweise veranlaßt durch einen von der Anwendung 5x bzw. vom Browser 33 übertragenen Steuercode, den digitalisierten Sprachstrom in Form eines Bitstrings an die zuständige Anwendung, z.B. 5x, weiter. Diese extrahiert aus dem empfangenen Bitstring die persönlichen Sprachmerkmale und vergleicht diese mit z. B. auf Plattenspeichern 60 abgelegten Referenzmustern 6x, um die Identität des Benutzers anhand seiner Sprechproben zu verifizieren.

Die Erfindung schließt auch ein, daß im Rahmen einer Rechnernwendung 34 von einem Internet-Server in den Rechner 30 geladene Daten, wie z. B. Telefonlisten, Adressenlisten, Umsatzdaten, Preislisten, in den Speicher 18 des Mobilfunktelefons 10 geladen und auf der Anzeige 15 dargestellt werden können, wobei durch die Tastatur 16 eine Auswahl möglich ist.

Bei einer weiteren Rechneranwendung 34 können am Mobilfunktelefon 10 eingetastete oder eingesprochene, digitalisierte Daten in den Rechner 30 übertragen und dort oder in einem Netzserver weiterverarbeitet bzw. später oder von anderen Personen abgerufen werden.

Weiterhin ist es möglich, daß - angestoßen durch eine Rechneranwendung 34 - über die Anschlußschnittstelle 31/12 in den Speicher 18 des Mobilfunktelefons 10 Programme geladen werden können, die in der Steuereinheit 11 zeitlich entkoppelt zum Ablauf gebracht werden können.

Schließlich können auch Anwendungen/Schlüssel - angestoßen durch eine Rechneranwendung 34 - auf der Chipkarte selbst geändert, gelöscht oder geladen werden.

In allen Fällen kann die Übertragung von Daten, Programmen oder Anwendungen zwischen dem Mobilfunktelefon 10 bzw. der Chipkarte 14/14a und dem Rechner 30 bzw. dem Netzserver integritätsgesichert oder verschlüsselt erfolgen. Die hierfür notwendigen Schlüssel sind entweder auf der Chipkarte bereits gespeichert oder werden vorher zwischen Rechner-/Netzserver-Anwendung und Chipkarte z. B. nach dem Diffie-Hellman-Verfahren ausgetauscht. Darüberhinaus kann das Mobilfunktelefon 10 ganz allgemein in analoger Weise für die Verschlüsselung bzw. Entschlüsselung von Daten verwendet werden.

Eine weitere Ausprägung der Erfindung besteht in der gemeinsamen Nutzung einer Chipkartenanwendung in GSM - und Festnetzen. Ein Beispiel hierfür ist die elektronische Geldbörse. Sie kann z. B. als Anwendung 14x auf der im Mobilfunktelefon 10 eingelegten Chipkarte 14/14a über eine Rechner-/Netz-Anwendung 33/34/5x aufgeladen werden und später während eines GSM-Telefongespräches, z. B. durch einen von der Funkvermittlungszentrale gesendeten Impuls in regelmäßigen Zeitabständen - entsprechend den entfernungsabhängigen Tarifen - dekrementiert werden. Derartiges „vorausbezahltes" Telefonieren redu-

ziert das Betrugsrisiko, dem Mobilfunkbetreiber heute vielfach ausgesetzt sind, erheblich.

Analoges gilt für vergleichbar ausgestattete andere Geräte mit Chipkarteneinheit, wie z.B. Fernsteuerungen im Bezahlfernsehen.

Patentansprüche

1. Gerät(10) der Telekommunikations- und/oder Fernsteuertechnik mit Chipkarteneinheit (13) für eine Chipkarte (14,14a) als Berechtigungsnachweis des Benutzers und Einrichtungen(12) zur Kopplung mit einem Rechner (30), dadurch gekennzeichnet, daß das Gerät (10) bei Verwendung entsprechender Chipkarten (14a) als Kartenterminal für den Rechner (30) zum Authentisierungs- und Berechtigungsnachweis bei der Inanspruchnahme von auf dem Rechner verfügbaren Diensten verwendbar ist.

2. Gerät(10) nach Anspruch 1 mit angekoppeltem Rechner (30), dadurch gekennzeichnet, daß der Rechner (30) unabhängig vom Gerät (10) an ein Kommunikationsnetz (40) angeschlossen ist und daß das Gerät(10) als angeschlossenes Kartenterminal arbeitend für die Inanspruchnahme von Netzdiensten in dem Kommunikationsnetz (40) verwendbar ist.

3. Gerät nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß alle für die Nutzung des Gerätes vorhandenen Bauteile mit einer Steuereinheit (11) verbunden sind, so daß Eingaben über eine Tastatur (16) oder ein Mikrofon speicherbar und über die Schnittstelle (12) weiterleitbar sind bzw. über die Schnittstelle (12) ankommende Daten speicherbar und/oder auf einer Anzeige (15) anzeigbar sind, wobei die anzuzeigenden Daten durch die Tastatur (16) auswählbar sind.

4. Verfahren zum Betreiben einer aus Gerät(10) mit gekoppeltem Rechner (30) bestehenden Gerätekombination nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß vor Inanspruchnahme von ein Kartenterminal erfordernden Netzdiensten zunächst der die Rechnerschnittstelle (31) für

das Gerät (10) steuernde Treiber (32) mit der benötigten Treibersoftware geladen wird.

5. Verfahren nach Anspruch 4,
dadurch gekennzeichnet,
daß die Bereitstellung der Treibersoftware durch eine von einer Anwendung (z.B. 14x) auf der Chipkarte (14,14a) signierte Anforderung erfolgt.

6. Verfahren nach Anspruch 4 oder 5 in Verbindung mit einem Mobilfunktelefon als Gerät,
dadurch gekennzeichnet,
daß die Treibersoftware über das Kommunikationsnetz (40) von einem Server des Mobilfunknetz-Betreibers auf Anforderung in den Treiber (32) des Rechners (30) geladen wird und daß anhand der Signierung der Treibersoftware mit einem privaten Schlüssel in Verbindung mit dem zugehörigen öffentlichen Schlüssel auf der Chipkarte (14/14a) das Vorliegen der authentischen Treibersoftware automatisch überprüft wird.

7. Verfahren nach einem der Ansprüche 4 bis 6,
dadurch gekennzeichnet,
daß nach Aufbau einer Verbindung vom Rechner (30) aus über das Kommunikationsnetz (40) zu einem Dienstanbieter (50) in Verbindung mit dem Gerät (10) als Kartenterminal Chipkartenanwendungen auswählbar und ausführbar sind.

8. Verfahren nach Anspruch 7,
dadurch gekennzeichnet,
daß das Gerät (10) als Kartenterminal des Rechners (30) zur Verschlüsselung von sensiblen Daten verwendet wird.

9. Verfahren nach Anspruch 7 oder 8,
dadurch gekennzeichnet,
daß im Rahmen einer laufenden Anwendung benötigte hochsensible Daten wie persönliche Geheimzahl (PIN) oder Geldbeträge

über die Tastatur (16) des Gerätes (10) eingegeben und von der Steuereinheit (11) in Verbindung mit der Chipkarte (14,14a) verschlüsselt weitergeleitet werden.

10. Verfahren nach Anspruch 7 oder 8,
dadurch gekennzeichnet,
daß als Berechtigungsnachweis oder zur Kontrolle auch über ein Mikrofon eingegebene Kontrollwörter an die Kontrollinstanz der eröffneten Anwendung weitergeleitet werden, so daß in Verbindung mit hinterlegten Referenzmustern eine Verifizierung des Benutzers durchführbar ist.

11. Verfahren nach einem der Ansprüche 7 bis 10,
dadurch gekennzeichnet,
daß im Rahmen einer Anwendung vom Rechner (30) übernommene Daten an den Speicher (18) des Gerätes (10) weitergeleitet werden.

12. Verfahren nach Anspruch 11,
dadurch gekennzeichnet,
daß die vom Rechner (30) übertragenen Daten zur Änderung der Daten in einem Chip der Chipkarte (14,14a) dienen.

13. Verfahren nach Anspruch 12 in Verbindung mit einem Funktelefon als Gerät,
dadurch gekennzeichnet,
daß bei einer als Geldkarte dienenden Chipkarte (14,14a) die während einer Funkverbindung des Mobilfunktelefons (10) eintreffenden Gebührenimpulse eine Abbuchung des entsprechenden Geldbetrages bewirken.

1/1

FIG 1

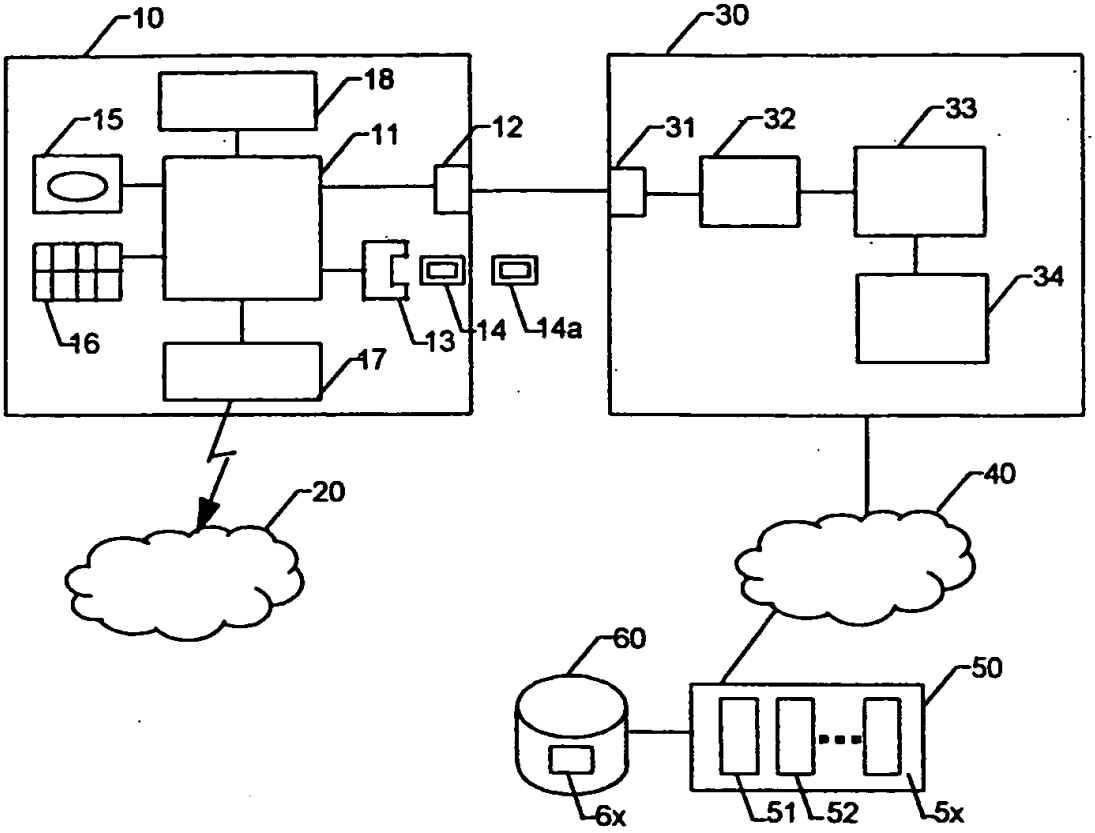
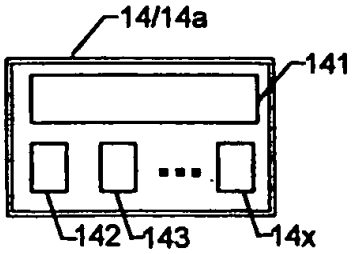

10
30
18
15
11
12
31
32
33
34
16
13
14
14a
17
20
40
60
50
6x
51
52
5x

FIG 2


14/14a
141
142
143
14x